

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-43152

(P2001-43152A)

(43) 公開日 平成13年2月16日 (2001.2.16)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 G 5 B 0 8 9 3 5 1 N 5 K 0 3 0
H 0 4 L 12/24 12/26 12/54		H 0 4 L 11/08 11/20	9 A 0 0 1 1 0 1 B

審査請求 未請求 請求項の数15 OL (全 24 頁) 最終頁に続く

(21) 出願番号 特願平11-213605

(22) 出願日 平成11年7月28日 (1999.7.28)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 五十嵐 政志

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(72) 発明者 鶴川 達也

東京都千代田区丸の内二丁目2番3号 三
菱電機株式会社内

(74) 代理人 100099461

弁理士 清井 章司 (外2名)

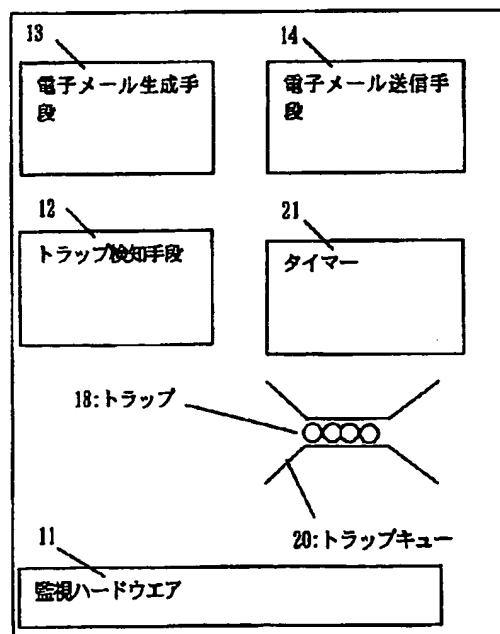
最終頁に続く

(54) 【発明の名称】 障害通知方式

(57) 【要約】

【課題】 障害を電子メールで通知する際にいくつかのトラップをまとめる事により送信する電子メールの数を減らし通信トラフィックを削減する。

【解決手段】 トラップ検知手段12は、監視ハードウェア11からトラップを受信した際にタイマー21が満了するまでの時間に受信した複数のトラップをトラップキュー20に溜めておき、タイマー21が満了したタイミングで、電子メール生成手段13によりトラップの内容を電子メールの本文に示す内容で作成し、電子メール送信手段14により、管理PCにメールを送信する。



実施の形態1の構成図

【特許請求の範囲】

【請求項1】 障害の発生を電子メールで通知する障害通知方式において、

コンピュータの状態を監視して監視した状態を示す状態情報を保持するとともに障害検出時に状態情報をトラップとして発生させる監視ハードウェアと、

上記監視ハードウェアが障害検出時に発生させるトラップを受信してトラップの発生を検知するトラップ検知手段と、

上記トラップ検知手段が受信した1つ以上のトラップをキューイングするトラップキューと、

上記トラップキューにキューイングされた1つ以上のトラップを含む電子メールを作成する電子メール生成手段と、

上記電子メール生成手段が作成した電子メールを送信する電子メール送信手段とを備えたことを特徴とする障害通知方式。

【請求項2】 上記障害通知方式は、さらに、上記トラップ検知手段がトラップを受信してから上記電子メール送信手段が電子メールを送信するまでの猶予時間として所定の時間を計測するタイマーを備え、

上記トラップキューは、上記タイマーが計測する所定の時間が経過するまで上記トラップ検知手段が受信した1つ以上のトラップをキューイングすることを特徴とする請求項1に記載の障害通知方式。

【請求項3】 上記トラップキューは、所定のトラップを発生させた障害の後処理の完了するまでの間に上記トラップ検知手段が受信する1つ以上のトラップをキューイングすることを特徴とする請求項1に記載の障害通知方式。

【請求項4】 上記障害通知方式は、さらに、上記タイマーが計測する所定の時間の値を、前回のトラップ発生から今回のトラップ発生までの経過時間に対応させて動的に決定するタイマー値決定手段を備えたことを特徴とする請求項2に記載の障害通知方式。

【請求項5】 上記障害通知方式は、さらに、上記トラップ検知手段が受信したトラップの回数を数えるカウンタを備え、上記トラップキューは上記カウンタの値が所定の上限値に達するまで上記トラップ検知手段が受信したトラップをキューイングすることを特徴とする請求項1に記載の障害通知方式。

【請求項6】 上記障害通知方式は、さらに、上記トラップ検知手段がトラップを受信してから上記電子メール送信手段が電子メールを送信するまでの猶予時間として所定の時間を計測するタイマーと上記トラップ検知手段が受信したトラップの回数を数えるカウンタとを備え、上記トラップキューは、上記タイマーが計測する所定の時間が経過するか、または、上記カウンタの値が所定の上限値に達するまでのいずれか一方を満足するまで、上記トラップ検知手段が受信した1つ以上のトラップをキ

ューイングすることを特徴とする請求項1に記載の障害通知方式。

【請求項7】 上記障害通知方式は、トラップの種類毎に重み付けされた値を予め保持し、トラップが発生する度に重み付けされた値を加算して合計値を算出し、算出した合計値が所定の障害合計値に達するまで上記トラップ検知手段が受信したトラップを上記トラップキューにキューイングさせる障害値加算手段を備えたことを特徴とする請求項1に記載の障害通知方式。

【請求項8】 上記障害通知方式は、複数の電子メール送信先を設定するとともに、設定された電子メール送信先毎に上記障害合計値を異ならせて設定可能な送信先テーブルを備え、上記トラップ検知手段は上記送信先テーブルを参照して、電子メール送信先毎に対応する障害合計値に達する毎に、電子メールを作成、送信させることを特徴とする請求項7に記載の障害通知方式。

【請求項9】 上記障害通知方式は、コンピュータが短い時間内に停止する可能性がある重障害に対応するトラップを予め登録する重障害トラップテーブルを備え、上記トラップ検知手段は受信したトラップが上記重障害トラップテーブルに登録されている場合に、電子メールを作成、送信させることを特徴とする請求項1から8いずれかに記載の障害通知方式。

【請求項10】 上記障害通知方式は、電子メールの送信先毎に送信するトラップを登録する送信トラップ登録テーブルと上記送信トラップ登録テーブルと電子メールの送信先との対応を定義する送信トラップ対応テーブルとを備えるとともに、

上記送信トラップ対応テーブルと上記送信トラップ登録テーブルとを参照して、電子メールの送信先毎に送信するトラップを選択して電子メール生成手段に電子メールを作成させるトラップ選別手段を備えたことを特徴とする請求項1～9いずれかに記載の障害通知方式。

【請求項11】 障害の発生を電子メールで通知する障害通知方式において、

コンピュータの状態を監視して監視した状態を示す状態情報を保持するとともに障害検出時に状態情報をトラップとして発生させる監視ハードウェアと、

上記監視ハードウェアが障害検出時に発生させるトラップを受信してトラップの発生を検知するトラップ検知手段と、

上記トラップ検知手段が受信した1つ以上のトラップをキューイングするトラップキューと、

上記トラップキューにキューイングされた1つ以上のトラップを含む電子メールを作成する電子メール生成手段と、

上記電子メール生成手段が作成した電子メールを送信する電子メール送信手段と、

上記トラップ検知手段が検知した1つのトラップの発生が一定の時間間隔以内に起こる状態が一定時間継続した

トラップ頻発状態を検出するトラップ頻発状態検出手段とを備え、

上記トラップ検知手段は、上記トラップ頻発状態検出手段がトラップ頻発状態を検出した際に、電子メールによる障害通知を一時停止するとともに、障害通知を一時停止したことを電子メールで監視者に伝えることを特徴とする障害通知方式。

【請求項12】 上記障害通知方式は、さらに、該トラップが発生しない状態が一定時間継続したことを検出するトラップ停止状態検出手段を備え、

上記トラップ検知手段は、上記トラップ停止状態検出手段がトラップ停止状態を検出した際に、電子メールによる障害通知を再開するとともに、障害通知を再開したことを電子メールで監視者に伝えることを特徴とする請求項11に記載の障害通知方式。

【請求項13】 上記障害通知方式は、さらに、頻発する可能性のある障害に対応するトラップを1つ以上記憶する頻発トラップ記憶手段を備え、

上記トラップ頻発状態検出手段は、上記頻発トラップ記憶手段が記憶するトラップのうちいずれか1つのトラップに関して、トラップ頻発状態を検出するとともに、

上記障害通知方式は、上記トラップ頻発状態が検出されたトラップに関して、電子メールによる障害通知を一時停止し、障害通知を一時停止したことを電子メールで監視者に伝えることを特徴とする請求項11に記載の障害通知方式。

【請求項14】 上記障害通知方式は、互いに関連する第1と第2のトラップの対と、上記第1と第2のトラップの対が連続して発生することが予想される所定の時間とを対応させて記憶するトラップ対記憶手段を備え、
上記トラップ検知手段は、上記トラップ対記憶手段を参照して、上記第1のトラップの発生を検知すると、上記所定の時間の経過、及び上記第2のトラップの発生のいずれかを待って、上記電子メール生成手段に対して電子メールを作成させ、作成した電子メールを上記電子メール送信手段により送信させることを特徴とする請求項11に記載の障害通知方式。

【請求項15】 上記第1のトラップは障害の発生を示す障害トラップであり、上記第2のトラップは該障害トラップに対応して自動的に発生する修復トラップであり、上記所定の時間は上記障害トラップに対して上記修復トラップの発生が期待される時間であって、
上記トラップ検知手段は、上記トラップ対記憶手段を参照して、上記第1のトラップの発生を検知すると、上記所定の時間の経過を待って、修復トラップが来ない場合に上記電子メール生成手段に対して電子メールを作成させ、作成した電子メールを上記電子メール送信手段により送信させることを特徴とする請求項14に記載の障害通知方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、例えば、ネットワークに接続されたコンピュータの障害監視に関するものである。また、例えば、障害の通知に電子メールを用いる障害通知方式に関するものである。

【0002】

【従来の技術】図29は、従来からある、電子メールによる障害通知方式を示す図である。図において、9aは監視される対象のコンピュータ（監視対象コンピュータ）であり、障害を自身で検出し電子メールで監視者に通知する。コンピュータ9aは、コンピュータ自身の状態を監視し状態情報を保持する監視ハードウェア91と、監視ハードウェア91が障害検出時に発生するトラップを受けるトラップ検知手段92と、トラップが示す障害情報を含む電子メールを作成する電子メール生成手段93と、作成した電子メールを送信する電子メール送信手段94を有する。コンピュータ9aより送信された電子メールは監視者の管理PC（Personal Computer）3aに送られる。2a、2bは電子メールがコンピュータ1aから管理PC3aに送られるまでに経由するメールサーバである。4a、4bは各々コンピュータ1a、管理PC3aの設置場所に敷設されたLAN（Local Area Network）、4cはそれらLAN同士を接続するLANまたはWAN（Wide Area Network）またはInternetである。

【0003】ここで、「監視ハードウェア」とは、ハードウェアやソフトウェアの障害を監視するコンピュータ本体とは独立したハードウェアであり、監視対象のソフトウェアやハードウェアの現在の状況に対応する変数を持ち、変数は「監視ハードウェア」内部の不揮発性のメモリに保持される。また「トラップ」とは、障害が発生した場合に監視ハードウェアから送られる、ハードウェアやソフトウェアの障害箇所を特定するための情報の事であり、「監視ハードウェア」が持つ変数のアドレスと値を含むデータから構成される。

【0004】次に、動作について説明する。コンピュータ9aの監視ハードウェア91が障害を検出すると、トラップ検知手段92に障害を示す情報であるトラップを送る。トラップ検知手段92はトラップを受け取ると電子メール生成手段93を呼んでトラップの内容を電子メールの形式にして、電子メールを作成し、さらに電子メール送信手段94を呼んで、今、電子メール生成手段93が作成した電子メールを管理PC3aに送信する。

【0005】ここで、トラップ検知手段92はトラップが発生する度に上述の動作を行う。従ってトラップの数と同じ数だけ電子メールが作成され、送信されることになる。コンピュータにある一つの障害が発生した場合、その事象に対応するトラップの数が一つであるとは限らず、一つの障害に対し複数の電子メールが送られる場合

もある。

【0006】

【発明が解決しようとする課題】従来の、電子メールによる障害通知方式は、以上のように構成されていたので、一つの事象に対して比較的短時間の間に複数のトラップが発生した場合、個々のトラップに対応して電子メールが送られるため、監視者は障害の全貌を掴むために、複数の電子メールを見る必要があるという問題があった。

【0007】また、電子メールは送信した順番に監視者に着信するとは限らず、特に送信間隔が短い場合は着信順序が狂う可能性が高い。このため、監視者が障害の全貌を掴むために重要となる、トラップの発生順序を特定することが困難となる問題があった。

【0008】また、コンピュータで異常状態が継続し、トラップが頻発あるいは連続発生した際、その都度、発生したトラップの数だけ、電子メールが送られ、メールサーバ、ネットワークに余計な負荷をかけてしまう問題があった。

【0009】この発明は、例えば、上記のような課題を解決するためになされたもので、複数のトラップが一つの電子メールにより送られ、監視者が障害の全貌を掴むのに複数の電子メールを見る必要が無いような障害通知方式を得ることを目的としている。また、例えば、電子メールに含まれるトラップの順序関係が一目瞭然で、監視者は容易にトラップの順序関係を知ることができる障害通知方式を得ることを目的としている。また、例えば、トラップ頻発および連続発生にてメールサーバ、ネットワークに余計な負荷をかけることのない、電子メールによる障害通知方式を得ることを目的とする。

【0010】

【課題を解決するための手段】この発明の障害通知方式は、障害の発生を電子メールで通知する障害通知方式において、コンピュータの状態を監視して監視した状態を示す状態情報を保持するとともに障害検出時に状態情報をトラップとして発生させる監視ハードウェアと、上記監視ハードウェアが障害検出時に発生させるトラップを受信してトラップの発生を検知するトラップ検知手段と、上記トラップ検知手段が受信した1つ以上のトラップをキューイングするトラップキューと、上記トラップキューにキューイングされた1つ以上のトラップを含む電子メールを作成する電子メール生成手段と、上記電子メール生成手段が作成した電子メールを送信する電子メール送信手段とを備えたことを特徴とする。

【0011】上記障害通知方式は、さらに、上記トラップ検知手段がトラップを受信してから上記電子メール送信手段が電子メールを送信するまでの猶予時間として所定の時間を計測するタイマーを備え、上記トラップキューは、上記タイマーが計測する所定の時間が経過するまで上記トラップ検知手段が受信した1つ以上のトラップ

をキューイングすることを特徴とする。

【0012】上記トラップキューは、所定のトラップを発生させた障害の後処理の完了するまでの間に上記トラップ検知手段が受信する1つ以上のトラップをキューイングすることを特徴とする。

【0013】上記障害通知方式は、さらに、上記タイマーが計測する所定の時間の値を、前回のトラップ発生から今回のトラップ発生までの経過時間に対応させて動的に決定するタイマー値決定手段を備えたことを特徴とする。

【0014】上記障害通知方式は、さらに、上記トラップ検知手段が受信したトラップの回数を数えるカウンタを備え、上記トラップキューは上記カウンタの値が所定の上限値に達するまで上記トラップ検知手段が受信したトラップをキューイングすることを特徴とする。

【0015】上記障害通知方式は、さらに、上記トラップ検知手段がトラップを受信してから上記電子メール送信手段が電子メールを送信するまでの猶予時間として所定の時間を計測するタイマーと上記トラップ検知手段が受信したトラップの回数を数えるカウンタとを備え、上記トラップキューは、上記タイマーが計測する所定の時間が経過するか、または、上記カウンタの値が所定の上限値に達するまでのいずれか一方を満足するまで、上記トラップ検知手段が受信した1つ以上のトラップをキューイングすることを特徴とする。

【0016】上記障害通知方式は、トラップの種類毎に重み付けされた値を予め保持し、トラップが発生する度に重み付けされた値を加算して合計値を算出し、算出した合計値が所定の障害合計値に達するまで上記トラップ検知手段が受信したトラップを上記トラップキューにキューイングさせる障害値加算手段を備えたことを特徴とする。

【0017】上記障害通知方式は、複数の電子メール送信先を設定するとともに、設定された電子メール送信先毎に上記障害合計値を異ならせて設定可能な送信先テーブルを備え、上記トラップ検知手段は上記送信先テーブルを参照して、電子メール送信先毎に対応する障害合計値に達する毎に、電子メールを作成、送信させることを特徴とする。

【0018】上記障害通知方式は、コンピュータが短い時間内に停止する可能性がある重障害に対応するトラップを予め登録する重障害トラップテーブルを備え、上記トラップ検知手段は受信したトラップが上記重障害トラップテーブルに登録されている場合に、電子メールを作成、送信させることを特徴とする。

【0019】上記障害通知方式は、電子メールの送信先毎に送信するトラップを登録する送信トラップ登録テーブルと上記送信トラップ登録テーブルと電子メールの送信先との対応を定義する送信トラップ対応テーブルとを備えるとともに、上記送信トラップ対応テーブルと上記

10

20

30

40

50

送信トラップ登録テーブルとを参照して、電子メールの送信先毎に送信するトラップを選択して電子メール生成手段に電子メールを作成させるトラップ選別手段を備えたことを特徴とする。

【0020】障害の発生を電子メールで通知する障害通知方式において、コンピュータの状態を監視して監視した状態を示す状態情報を保持するとともに障害検出時に状態情報をトラップとして発生させる監視ハードウェアと、上記監視ハードウェアが障害検出時に発生させるトラップを受信してトラップの発生を検知するトラップ検知手段と、上記トラップ検知手段が受信した1つ以上のトラップをキューイングするトラップキューと、上記トラップキューにキューイングされた1つ以上のトラップを含む電子メールを作成する電子メール生成手段と、上記電子メール生成手段が作成した電子メールを送信する電子メール送信手段と、上記トラップ検知手段が検知した1つのトラップの発生が一定の時間間隔以内に起こる状態が一定時間継続したトラップ頻発状態を検出するトラップ頻発状態検出手段とを備え、上記トラップ検知手段は、上記トラップ頻発状態検出手段がトラップ頻発状態を検出した際に、電子メールによる障害通知を一時停止するとともに、障害通知を一時停止したことを電子メールで監視者に伝えることを特徴とする。

【0021】上記障害通知方式は、さらに、該トラップが発生しない状態が一定時間継続したことを検出するトラップ停止状態検出手段を備え、上記トラップ検知手段は、上記トラップ停止状態検出手段がトラップ停止状態を検出した際に、電子メールによる障害通知を再開するとともに、障害通知を再開したことを電子メールで監視者に伝えることを特徴とする。

【0022】上記障害通知方式は、さらに、頻発する可能性のある障害に対応するトラップを1つ以上記憶する頻発トラップ記憶手段を備え、上記トラップ頻発状態検出手段は、上記頻発トラップ記憶手段が記憶するトラップのうちいずれか1つのトラップに関して、トラップ頻発状態を検出するとともに、上記障害通知方式は、上記トラップ頻発状態が検出されたトラップに関して、電子メールによる障害通知を一時停止し、障害通知を一時停止したことを電子メールで監視者に伝えることを特徴とする。

【0023】上記障害通知方式は、互いに関連する第1と第2のトラップの対と、上記第1と第2のトラップの対が連続して発生することが予想される所定の時間とを対応させて記憶するトラップ対記憶手段を備え、上記トラップ検知手段は、上記トラップ対記憶手段を参照して、上記第1のトラップの発生を検知すると、上記所定の時間の経過、及び上記第2のトラップの発生のいずれかを待って、上記電子メール生成手段に対して電子メールを作成させ、作成した電子メールを上記電子メール送信手段により送信させることを特徴とする。

【0024】上記第1のトラップは障害の発生を示す障害トラップであり、上記第2のトラップは該障害トラップに対応して自動的に発生する修復トラップであり、上記所定の時間は上記障害トラップに対して上記修復トラップの発生が期待される時間であって、上記トラップ検知手段は、上記トラップ対記憶手段を参照して、上記第1のトラップの発生を検知すると、上記所定の時間の経過を待って、修復トラップが来ない場合に上記電子メール生成手段に対して電子メールを作成させ、作成した電子メールを上記電子メール送信手段により送信させることを特徴とする。

【0025】

【発明の実施の形態】以下、この発明の実施の形態を説明する。

実施の形態1. この実施の形態、および以降の実施の形態における、システム全体の構成は、従来の図29に示す構成と同じである。この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、電子メールを作成、送信するまでの猶予時間を与えるタイマーと、猶予時間内に受信したトラップをキューイングするトラップキューとをコンピュータ上に備えたものである。以下に、図を用いて説明する。

【0026】図1は、実施の形態1によるコンピュータの構成を示す図である。図1においては、コンピュータの状態を監視し、状態情報を保持する監視ハードウェア11と、監視ハードウェアからのトラップを受信するトラップ検知手段12と、受信したトラップを元に電子メールを作成する電子メール生成手段13と、作成した電子メールを監視者に送信する電子メール送信手段14は、従来の図29に示す構成の監視ハードウェア91～電子メール送信手段94にそれぞれ相当する。

【0027】前述したように、「監視ハードウェア」とは、ハードウェアやソフトウェアの障害を監視するハードウェアであり、コンピュータ本体とは独立したハードウェアである。「監視ハードウェア」は、監視対象のソフトウェアやハードウェアの現在の状況に対応する変数を持つ。具体的には、監視情報を「変数アドレスと値」という形式で「監視ハードウェア」内部の不揮発性のメモリに保持している。このように、不揮発性メモリ上に保持された「変数アドレスと値」情報そのものを状態情報と呼ぶ。また「トラップ」とは、障害が発生した場合に監視ハードウェアから送られる、ハードウェアやソフトウェアの障害箇所を特定するための情報の事である。「トラップ」は、「監視ハードウェア」が持つ変数のアドレスと値を含むデータから構成される。監視ハードウェア11が不揮発性メモリ上に持つ変数のアドレスと値を含むデータは、トラップとして監視ハードウェア11からトラップ検知手段12に送られる。トラップ検知手段12は、必要に応じて、トラップを検知する。即ち、

自分が知りたい情報以外は無視することもあるが、自分が知りたい情報は取り入れて、トラップを検知する。

【0028】図1の20は監視ハードウェア11から送られてきたトラップ18の発生順序を保ったままトラップ18を保管しておくトラップキュー、21はトラップ検知手段12が最初のトラップを受信してから電子メールを作成、送信するまでの猶予時間を与えるために時間を計測するタイマーである。

【0029】次に、動作について説明する。図2は、トラップ検知手段12がトラップ18を受信してから電子メール送信手段14により電子メールを送信するまでの処理を示すフローチャートである。ステップST101において、トラップ検知手段12は監視ハードウェア11からトラップを受信するまで待機しており、トラップを受信すると、以下の処理を行なう。ステップST102でトラップ検知手段12は予め決められたタイマー値でタイマー21を起動する。タイマー値としては、例えば、何らかの固定値をセットしておけばよい。固定値はプログラムで設定しておいてもよいし、システムのインストール時に設定してもよい。次に、ステップST103でトラップ検知手段12は、今受信したトラップ18をトラップキュー20に追加する。その後、ステップST104にて、イベント待ち状態となり、次のトラップ発生のイベント、またはタイマー満了のイベントを待つ。

【0030】ステップST104のイベント待ち状態で監視ハードウェア11から再びトラップを受信する場合の処理の流れを説明する。まず、ステップST105で、イベント発生を検知し、ステップST106でイベントの種類がトラップ発生か、タイマー満了かを判断する。ここでは、イベントの種類がトラップ発生なので、ステップST107でトラップをトラップキュー20に追加し、再びステップST104に戻り、次のイベントを待つ。トラップ18を受信する度にこの操作を繰り返し、その都度トラップ18がトラップキュー20に追加されていく。

【0031】次に、タイマー満了の場合の処理の流れを説明する。ステップST104のイベント待ち状態でタイマー21が満了すると、トラップ検知手段12は、ステップST108において、電子メール生成手段13により、トラップキュー20に蓄えられた全てのトラップ情報を順番に反映した電子メールを作成する。即ち、トラップは、発生順にキューイングされ、キューイングされた順番で電子メール本文に記載される。次に、ステップST109でトラップ検知手段12はトラップキューをクリアする。最後に、ステップST110において、電子メール送信手段14により監視者に電子メールを送信する。なお、ステップST109のトラップキュー20のクリアと、ステップST110の電子メール送信は、順序を入れ替えて実行してもかまわない。

【0032】なお、監視者に送信される電子メールの内容を図3に示す。発生した時刻の順番でトラップの発生時刻62、変数アドレス63、変数値64が書き込まれている。変数アドレス63と変数値64の組み合わせがトラップであり、そのトラップの発生時刻62とともに電子メールの本文の内容として書かれている。監視者には、トラップ毎の変数アドレスと変数値の組み合わせにより、どのような障害、事象が発生したかを示す対応表が別途提供されており、監視者はその対応表と電子メールの内容を照らし合わせるにより、コンピュータにどのような障害、事象が、どのような経緯で発生したかを知ることができる。対応表は、予め提供されているか、あるいは電子メールと並行して提供されているものとする。いずれにしても、電子メール到着時（解析時）に監視者の手元にあればよい。

【0033】この実施の形態では、監視ハードウェアによりコンピュータの状態を監視し状態情報を保持する機能を有するコンピュータにおいて、発生した障害の内容を電子メールで監視者に通知する際に、障害によるトラップ発生後すぐに電子メールを送信せず、一定時間待ち、その間に検出した複数のトラップをまとめて一つの電子メールで監視者に送信することを特徴とする障害通知方式について説明した。

【0034】以上のように、この実施の形態によれば、トラップ受信後タイマー猶予時間待ってから電子メールが送られるため、複数のトラップが短い時間内に連続で発生しても電子メールが複数送られることなく、メールサーバ、ネットワークに余計な負荷をかけることが無いという効果が得られる。またトラップキューを用いているため、電子メールに含まれるトラップの発生順序が失われずに監視者に通知され、監視者の解析を容易にする効果が得られる。

【0035】また、上述した本実施の形態では、猶予時間として予め決めた固定時間を用いているが、それ以外にトラップ受信後の後処理時間を利用することもできる。トラップ受信後の後処理時間とは、トラップを発生させた障害に伴い、コンピュータシステムで行なわれる処理にかかる時間である。ここで、トラップ発生後の後処理とは、データベース停止などコンピュータ上のアプリケーションの緊急停止処理、障害情報の電光掲示板表示、警報ランプ点灯、監視ハードウェアの持つ状態情報のダンプ等のことである。このような時間、例えば、アプリケーションの停止にかかる時間、トラップの発生を電光掲示板に表示する処理にかかる時間、トラップの発生により警報ランプを点灯する処理にかかる時間、監視ハードウェア11が保持するコンピュータの全状態情報をダンプするためにかかる時間などが、猶予時間として利用できる。これらのトラップ発生後の後処理の時間は、例えば、予め、トラップ検知手段内部など、所定の記憶部に各トラップに対応させて時間を記憶しておき、

検出したトラップに対応する時間をタイマーにセットしてもよい。

【0036】即ち、この発明の実施の形態の他の例に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、その後処理をする間、電子メールの作成、送信を控え、その間に受信したトラップをキューイングするトラップキューをコンピュータ上に備えたものである。

【0037】以上のように、この実施の形態の他の例として、上記コンピュータにおいて、障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、トラップ発生後の後処理が完了する間待ち、その間に発生したトラップと一まとめにして一つの電子メールで監視者に送信することを特徴とする障害通知方式について説明した。

【0038】本実施形態には、さらに次のような改良を加えることができる。ここまで説明した実施例では、タイマーによる猶予時間が固定であったため、以下のような問題がある。まず、障害に関連するトラップの発生が単独で、発生間隔が猶予時間に比べ十分に長い場合、猶予時間待っても待たなくても、メールサーバ、ネットワークにかかる負荷に相違は無く、むしろトラップ発生後猶予時間待つだけ、通知の即時性が失われることとなる。逆にトラップが短時間に連続して発生する場合は、猶予時間待って電子メールを送信しても、その後トラップが続くようであれば、同じ猶予時間後に再度電子メールを送ることになり、このトラップの連続発生を一つの障害、事象として捉えたい監視者に対して、複数のメールに分割されて電子メールが送られ、解析をし難くすることになる。

【0039】この問題点を解決するために、以下の方法でタイマー21による猶予時間を動的に変更できるようにする。

【0040】この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、電子メールを作成、送信するまでの猶予時間を与えるタイマーと、猶予時間内に受信したトラップをキューイングするトラップキューとをコンピュータ上に備え、さらに猶予時間として、前回のトラップ発生からの経過時間に対応する時間、例えば、前回のトラップ発生からの経過時間に反比例する値を動的に決定する、タイマー値決定手段を備えたものである。

【0041】図4は、図1に示した本実施の形態におけるコンピュータの構成に、トラップを受信した時に前回のトラップ発生からの経過時間をパラメータとして、猶予時間を動的に決定し、決定した猶予時間を用いてタイマー21を起動することができる、タイマー値決定手段22を新たに有するものである。また、前回のトラップ発生からの経過時間を求めるために、前回のトラップ発

生の時刻を記憶する時刻記憶手段15を有するものである。これによりトラップの発生がまばらで猶予時間による通知の即時性が失われることが懸念される場合はタイマー値を短くし、逆にトラップが短時間に集中し、猶予時間により電子メールが分割されてしまうことが懸念される場合はタイマー値を長くすることができる。

【0042】以下に、タイマー値決定の処理の一例について、具体的に述べる。図4に示した構成を採る場合の処理は、図2のフローチャートのステップST102のタイマー起動の処理において、例えば、図5に示すフローチャートで示されるタイマー値決定の処理を行なう。

【0043】タイマー値決定手段22がタイマー値を決定する方法について、図5を用いて説明する。ステップST111でトラップが発生すると、ステップST112で時刻記憶手段15に記憶された前回のトラップ発生時刻と今回発生したトラップの発生時刻から経過時間を計算する。ステップST113でこの経過時間を元に、予め決めておいた固定値パラメータに対し反比例するタイマー値を算出する。例えば経過時間30分、固定値パラメータを15（分）とすると、

固定値パラメータ÷経過時間＝タイマー値に従い
 $15 \div 30 = 0.5$ となり、

次のタイマー値は0.5分となる。

【0044】ここで経過時間からタイマー値を求めるのに反比例関係を利用する代わりに、両者の合計値が常に一定である関係を利用しても良い。その時の計算式は、経過時間＋タイマー値＝固定値となる。

【0045】このようにタイマー値を決めると、トラップの発生間隔がまばらな間（長い間）はタイマー値が短くなり、トラップの発生間隔が短い場合はタイマー値が長くなるが、場合によってはタイマー値が極端に長くなったり、短くなったりする場合は発生する。経過時間とタイマー値の合計値が一定である関係を利用してタイマー値を設定すると、タイマー値がマイナスになることもあり得る。このような場合の対策として、予めタイマー値の上限値と下限値を設けておき（例えば上限値を5分、下限値を5秒とする）、ステップST114、ステップST115で経過時間から算出されたタイマー値と予め設けられた下限値および上限値との比較を行い、算出されたタイマー値が下限値よりも小さければ下限値を次のタイマー値として採用する（ステップST118）、算出されたタイマー値が上限値よりも大きければ上限値を次のタイマー値として採用する（ステップST116）、算出されたタイマー値が両者の間に入っていれば、そのままその値を次のタイマー値として採用する（ステップST117）ようにする。タイマー値が決まったらステップST119にてタイマーを起動する。

【0046】このように構成することにより、トラップ

の発生がまばらな間は猶予時間が小さくなり、猶予時間をおくことにより通知の即時性が失われることを防ぐ効果が得られ、逆にトラップが短い時間間隔で連続発生する場合は、猶予時間が長くなり、監視者にメールが分割されて送られ難くなる効果が得られる。

【0047】以上のように、この実施の形態では、上記コンピュータにおいて、発生した障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、ある一定時間待ち、その間に検出した複数のトラップをまとめて一つの電子メールで監視者に送信する構成において、トラップが発生した際に、前回の障害発生からの経過時間を記録しておき、その時間に反比例する時間を電子メール送信までの待ち時間として採用することを特徴とする障害通知方式について説明した。

【0048】実施の形態2. これまでに説明した実施の形態1では、監視ハードウェア11からトラップを受信した後、猶予時間を定めて、猶予時間の間のトラップを溜めた後で電子メールを送信する形態としていた。この方法では1通の電子メールで送る事のできるトラップの数に制限はないため、猶予時間の間に来たトラップが多い場合には非常にデータ量の大きな電子メールを送信する事になる。あまりに大きい電子メールは中継するメールサーバをダウンさせる可能性がある。この実施の形態はこの問題を解消するものである。

【0049】この実施の形態におけるシステム全体の構成は、従来の図29に示す構成と同じである。この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、電子メールを作成、送信するまでのトラップ回数を数えるカウンタと、猶予時間内に受信したトラップをキューイングするトラップキューとをコンピュータ上に備えたものである。

【0050】図6は実施の形態2によるコンピュータの構成を示す図である。図6において、コンピュータの状態を監視し、状態情報を保持する監視ハードウェア11と、監視ハードウェアからのトラップを受信するトラップ検知手段12と、受信したトラップを元に電子メールを作成する電子メール生成手段13と、作成した電子メールを監視者に送信する電子メール送信手段14とトラップキュー20は、実施の形態1の図1に示す構成と同じである。図6の30はトラップの受信のたびに"1"が加算されるカウンタである。カウンタの値は、例えば、トラップ検知手段が保持する上限値と比較される。

【0051】次に、動作について説明する。図7は、トラップ検知手段12がトラップを受信してから電子メールを送信するまでの処理を示すフローチャートである。ステップST120において、トラップ検知手段12は監視ハードウェア11からトラップを受ける。ステップST121でカウンタ30を"1"で初期化し、ステッ

プST122で今受信したトラップをトラップキュー20に追加する。その後、ステップST123にてトラップ発生のイベントを待つ。

【0052】ステップST123でトラップを受信するとステップST124でトラップをトラップキュー20に追加する、そして、ステップST125でカウンタ30に"1"を加える。そして、ステップST126でカウンタ30が上限値を超えたかどうかを判断して超えていない場合には、ステップST123の処理に戻りトラップ発生のイベントを待機する。

【0053】ステップST126でカウンタ30が上限値を超えた場合には、ステップST127において電子メール生成手段13はトラップキュー20に蓄えられた全てのトラップ情報を順番に反映した電子メールを作成し、ステップST128でトラップキューをクリアする。最後にステップST129において、電子メール送信手段14が監視者に電子メールを送信する。そして、ステップST120に戻りトラップ検知手段12が再びトラップを受信するまで待機する。

【0054】以上のようにこの実施の形態2によれば、トラップが一定の数たまってから電子メールが送られるため、1通の電子メールに含まれるトラップの数は一定の数になり、多くのトラップを含む、極端にデータ量の大きなメールにより中継するメールサーバをダウンさせる危険を防ぐ事ができる。また、1つのトラップごとに電子メールを送信せず、複数のトラップがまとめて送信されるためメールサーバ、ネットワークに余計な負荷をかけることが無いという効果が得られる。またトラップキューを用いているため、電子メールに含まれるトラップの発生順序が失われずに監視者に通知され、監視者の解析を容易にする効果が得られる。送信される電子メールの内容は図3に示すものと同じである。

【0055】以上のように、この実施の形態では、上記コンピュータにおいて、障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、トラップの数が一定の個数溜まってから複数のトラップをまとめて一つの電子メールで監視者に送信することを特徴とする障害通知方式について説明した。

【0056】また、実施の形態2はさらに以下の改良を加える事ができる。ここまで説明した実施例では、トラップの数が上限に達するまで電子メールを送信する事がないため、トラップの数が上限より少ない数で治まる障害が発生するといつまでも障害通報の電子メールが送信されない。これを防ぐために上限を低くすると、多くのトラップが発生する障害が発生した場合に、電子メールの数が増加して、メールサーバ、ネットワークへの負荷が増大し、また1つの障害が複数の電子メールに分割される数が多くなるため解析が難しくなるという問題点が生ずる。

【0057】この問題点を解決するために、トラップの

数を数えるカウンタの他に、一定の猶予時間経過後には電子メールを送信するためのタイマーを加えた構成を考える。

【0058】この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、電子メールを作成、送信するまでの猶予時間を与えるタイマーと、電子メールを作成、送信するまでのトラップ回数を数えるカウンタと、猶予時間内に受信したトラップをキューイングするトラップキューとをコンピュータ上に備えたものである。

【0059】図8は、図6の実施の形態2におけるコンピュータの構成に、タイマー21を新たに有するものである。これにより、トラップの数が上限に達していない場合でも、猶予時間の経過後には電子メールが送信されて、上限より少ないトラップが発生する障害の場合にも猶予時間経過後には電子メールを送信する事ができる。

【0060】次に、図8に示す障害通知方式の動作について説明する。図9は、図8において、トラップ検知手段12がトラップを受信してから電子メールを送信するまでの処理を示すフローチャートである。ステップST130において、トラップ検知手段12は監視ハードウェア11からトラップを受ける。ステップST131でトラップ検知手段12は予め決められたタイマー値でタイマー21を起動し、ステップST132でカウンタ30を"1"で初期化し、ステップST133で今受信したトラップをトラップキュー20に追加する。その後、ステップST134にてトラップ発生イベントまたはタイマー満了のイベントを待機する。

【0061】ステップST134のイベント待ち状態で監視ハードウェア11から再びトラップを受信する場合の処理の流れを説明する。まず、ステップST134で、イベント発生を検知し、ステップST135で、イベントの種類がトラップ発生か、タイマー満了かを判断する。ここでは、イベントがトラップ発生なので、ステップST136でトラップをトラップキュー20に追加し、ステップST137でカウンタ30に"1"を加える。そして、ステップST138でカウンタ30が上限を超えたかどうかを判断する。超えていない場合には、Noとなり、ステップST134に戻りトラップ発生、または、タイマー満了のイベントを待機する。

【0062】ステップST134、ST135のイベント待ち状態でタイマーが満了した場合、あるいは、監視ハードウェア11から再びトラップを受信して、ステップST137でカウンタ30に"1"を加えた時にカウンタが上限値に達した場合には、ST138の判断でYesとなり、ST139で電子メール生成手段により電子メール本文61が作成される。その後、ステップST140でトラップキューをクリアしてステップST141で電子メール送信手段により電子メールを監視者に送

信する。なお、ステップST140のトラップキューのクリアは、ステップST141のメール送信のあとで実行してもよい。

【0063】この実施の形態によれば、障害通報の電子メールに含まれるトラップの数は上限より多くなる事はないため、極端に大きな電子メールが送信される事がなく、また、トラップの数が上限に達しない場合にも一定の時間の経過後に障害内容をまとめた電子メールを送信できるという効果を得る事ができる。

【0064】以上のように、この実施の形態では、上記コンピュータにおいて、発生した障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、トラップの数が一定の個数溜まった場合、あるいは、一定の時間経過した場合のいずれかの条件を満たすまでの複数のトラップをまとめて1つの電子メールで監視者に送信する事を特徴とする障害通知方式について説明した。

【0065】実施の形態3. これまでに説明した実施の形態1、2では、トラップ検知手段12が、監視ハードウェア11からトラップを受信した後、そのトラップの内容には関わり無く、猶予時間、あるいはトラップの滞留個数を定義して、ある程度トラップを溜めた後電子メールを送信する形態としていたため、早急に監視者に伝えるべき重大な障害を示すトラップが発生したとしても、ある程度時間が経たなければ電子メールが送られず、監視者への通知が遅れる場合がある。この実施の形態は、この問題を解消するものである。

【0066】この実施の形態におけるシステム全体の構成は、従来の図29に示す構成と同じである。この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した時、トラップがその重要度に応じた値を持っており、その値を加算し、合計値がある値に達したら電子メールを作成、送信する障害値加算手段と、加算されている間に受信したトラップをキューイングするトラップキューとをコンピュータ上に備えたものである。

【0067】図10は実施の形態3によるコンピュータの構成を示す図である。図10においても、コンピュータの状態を監視し、状態情報を保持する監視ハードウェア11と、監視ハードウェアからのトラップを受信するトラップ検知手段12と、受信したトラップを元に電子メールを作成する電子メール生成手段13と、作成した電子メールを監視者に送信する電子メール送信手段14とトラップキュー20は、実施の形態1の図1、実施の形態2の図6に示す構成と同じである。図10の41は、個々のトラップが持つその重大度を示す障害値を加算し、合計値を算出し、算出した合計値を保持する、障害値加算手段である。

【0068】次に、動作について説明する。図11は、トラップ検知手段12がトラップを受信してから電子メ

ールを送信するまでの処理を示すフローチャートである。ステップST142において、トラップ検知手段12は、監視ハードウェア11からのトラップ発生を待つ。トラップが発生するとステップST143でトラップ検知手段12がトラップを検出し、ステップST144でトラップをトラップキュー20に追加する。次にステップST145において、障害値加算手段41がトラップの障害値を加算し、合計値を保持する。合計値が予め決められた一定値を越えるまで、トラップが発生する度に以上の処理を繰り返す。ここで、トラップの障害値はその重大度に応じて、例えば"1"から"10"の10段階(10が最も重大な障害を示す)で予めトラップに割り当てられて、例えば、障害値加算手段41内に保持されているものとする。あるいは、障害値加算手段41から参照可能であれば、障害値加算手段41の外部に保持されていてもよい。

【0069】ステップST146で障害値加算手段41は、障害値合計が、予め決められた一定値を越えたか判断する。予め決められた一定値を超えると、ステップST147において電子メール生成手段13がトラップキュー20に蓄えられた全てのトラップ情報を順番に反映した電子メールを作成し、ステップST148でトラップキュー20をクリアする。ステップST149で障害値加算手段41が障害合計値をクリアし、最後にステップST150で電子メール送信手段14が監視者に電子メールを送信する。送信される電子メールの内容は図3に示すものと同じである。また、ステップST148のキュークリア、ST149の障害合計値クリア、ST150の電子メール送信は、順不同でよい。

【0070】この実施の形態3によれば、トラップの種類ごとにトラップの重大性、緊急度に応じて重み付けされた値(障害値)を持たせ、その障害値の合計によりメールの送信を判断する。このため、監視者に早く通知すべき重大なトラップが発生すると、その障害値が大きいのですぐに一定値を越えることとなり、監視者に早く通知が行われる効果が得られる。

【0071】なお、ここでは、障害値を1~10の10段階とする例を示したが、1~100等、他の値でも構わない。また、3段階、5段階など10より少ない段階にしてもよい。逆に、15段階、20段階など、段階を多く設定しても構わない。

【0072】以上のように、この実施の形態では、上記コンピュータにおいて、障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、トラップの種類毎の重大性、緊急度に応じて、重み付けされた値を持たせ、トラップが発生する度にその値を加算し、合計値が一定の値を越えてから複数のトラップをまとめて一つの電子メールで監視者に送信することを特徴とする障害通知方式について説明した。

【0073】次に、この実施の形態の変形例について説

明する。これまでは、監視者は一人であるという前提の元に、障害通知方式の説明をしてきたが、監視者の中にはローカルなシステム全体の管理を行い、障害が発生する度に処置を行う必要がある情シ部門(情報システム部門)の管理者や、全社のシステムを統合的に管理し、個々の障害に対する処置は行わないが、ローカルシステム毎の障害の発生状況は把握しておく必要がある管理者もいる。後者(以降「全社の管理者」と呼ぶ)は、前者(以降「情シ部門の管理者」と呼ぶ)程の頻度で電子メールが送られる必要は無く、ある程度障害の発生が溜まった段階で電子メールが送られれば十分である。

【0074】このような要求にも対応するために、本実施形態には、さらに次のような改良を加えることができる。即ち、複数の電子メール送信先を設定することができ、設定先毎に電子メールを作成、送信する障害合計値を変更することができるものである。図12は、この実施の形態におけるコンピュータの構成を示したものである。図12は、図10に新たに51の送信先テーブルが加わり、トラップキュー20が送信先テーブルのエントリ数分20a, 20b, . . . 20nまで増設されたものである。送信先テーブル51は監視者の電子メールアドレス512と、電子メールを送信する障害合計値513、現在の障害合計値514を保持するもので、複数のエントリを指定することができる。

【0075】次に、動作について説明する。図13は、トラップ検知手段12がトラップを受信してから電子メールを送信するまでの処理を示すフローチャートである。ステップST151において、トラップ検知手段12は、監視ハードウェア11からのトラップ発生を待つ。トラップが発生するとステップST152でトラップ検知手段12がトラップを受信して検出し、ステップST153でトラップを全てのトラップキュー20a, 20b, . . . 20nに追加する。次にステップST154において、障害値加算手段41が送信先テーブル51のエントリ毎に現在の障害合計値514欄に対応するトラップの障害値を加算し書き込む。ここでエントリ毎に電子メールを送信する障害合計値513と現在の障害合計値514を比較し(ST155)、現在の障害合計値514が電子メールを送信する障害合計値513を上回るものが無ければ、再びステップST151に戻り監視ハードウェアからのトラップを待つ。

【0076】ステップST155で現在の障害合計値514が、電子メールを送信する障害合計値513を越えるものが検出された場合は、それに該当するエントリ毎に以下の処理を行う(ST156)。ステップST157において、電子メール生成手段13がエントリに対応するトラップキューのデータを順番に反映した電子メールを作成し、ステップST158で対応するトラップキューをクリアする。ステップST159で障害値加算手段41がエントリに対応する現在の障害合計値514を

クリアし、最後にステップST160で電子メール送信手段14が監視者に電子メールを送信する。送信される電子メールの内容は図3に示すものと同じである。

【0077】このように、この実施の形態によれば、監視者（電子メールアドレス）毎に電子メールを送信する障害合計値を変えて登録できる送信先テーブルを設けたので、例えば、障害発生毎に処置の必要な情報システム部門の管理者には早く電子メールが送信され、迅速に処置が行えるようになるとともに、全社の管理者には障害がある程度まとまった段階で適切な頻度で電子メールが送信されるという効果が得られる。

【0078】以上のように、この実施の形態では、上記コンピュータにおいて、障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、トラップが発生する度に、予めトラップごとに設定してある値を加算し、合計値がある値（予め設定してある送信値）を越えた時に複数のトラップをまとめて一つの電子メールで監視者に送信する際に、送信先によりメールを送信する判断基準となる重み付けされた値の合計値を変化させられることを特徴とする障害通知方式について説明した。

【0079】実施の形態4。これまでに説明した実施の形態1、2、3ではトラップ検知手段12が監視ハードウェア11からトラップを受信した後、ある程度トラップを溜めた後で電子メールを送信する形態としていた。このため重障害が発生した場合は電子メールを送信する前にシステムがダウンする可能性があり、監視者へ通知が行なわれない可能性があった。実施の形態4はこの問題の発生を低減するものである。

【0080】この実施の形態におけるシステム全体の構成は、従来の図29に示す構成と同じである。この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、これまでに示した方法である程度障害を溜めてから一つの電子メールで監視者に送信する構成において、コンピュータが短い時間内に停止する可能性のある重障害を示すトラップが発生した場合は、その時の猶予時間、トラップ滞留個数の条件に満たなくとも、電子メールを送信するものである。コンピュータの構成は図1、図4、図6、図8、図10、図12の何れかに図14の52を加えた構成となる。52は重障害を示すトラップのテーブル（重障害トラップテーブル）である。

【0081】次に、動作について説明する。図15は、トラップ検知手段12がトラップを受信してから電子メールを送信するまでの処理を示すフローチャートである。ステップST301において、トラップ検知手段12は、監視ハードウェア11からのトラップ発生を待つ。トラップが発生するとトラップ検知手段12がトラップを検出し、ステップST303で検出したトラップ

が重障害トラップテーブルに存在するかどうか判断する。重障害トラップテーブルに存在する場合、Yesとなり、ステップST308で電子メール生成手段13がエントリに対応するトラップキューのデータを順番に反映した電子メールを作成し、ステップST309で該当するトラップキューをクリアする。最後にステップST310で電子メール送信手段14が監視者に電子メールを送信する。送信される電子メールの内容は図3に示すものと同じである。この場合、今回発生して検知された（重障害トラップテーブルに存在する）トラップが、電子メールの本文の最後に付くことになり、その前には、そのトラップ以前に、トラップキュー20にキューイングされていたトラップが並ぶことになる。

【0082】また、他のメール作成方法として、ステップST308では、今、検出されたトラップ（重障害トラップテーブルに存在するトラップ）だけを電子メール本文に作成してもいい。この場合、ステップST309のキューのクリアは行わず、まだ、管理者に送信していないトラップを残しておき、次のメールで送信するようにしてもよい。

【0083】また、ステップST303の判断で、検出したトラップが重障害トラップテーブルに存在しない場合、Noとなり、ここでのメール送信は行わず、ステップST305でトラップキューへの追加処理を行い、再びステップST301に戻り、監視ハードウェアからのトラップを待つ。トラップキューに追加する時の追加処理に付いては、例えば、この実施の形態以外の他の実施の形態で述べているようなトラップのキューへの追加処理を行なうものとする。

【0084】このように、実施の形態4ではトラップを受信した直後に、重障害を示すトラップのテーブル52を検索し、トラップのアドレスがテーブル内に存在した場合には、トラップキューの内容を元に電子メール本文を作成して、トラップキューをクリアして電子メールを送信する。

【0085】このようにする事により、重障害を示すトラップを受信した場合には、すぐに監視者に電子メールが送信され、重障害によるシステムダウンの前に通知できる可能性が高くなる効果が得られる。

【0086】以上のように、この実施の形態では、上記コンピュータにおいて、発生した障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、これまでに示した方法である程度トラップを溜めてから一つの電子メールで監視者に送信する構成において、コンピュータが短い時間内に停止する可能性のある障害が発生した場合は、電子メール送信待ち時間、滞留個数の条件に満たなくとも、電子メールを送信することを特徴とする障害通知方式について説明した。

【0087】実施の形態5。これまでに説明した実施の

形態では監視者が複数の場合にも全ての監視者に全てのトラップが送信された。しかし、トラップには、例えば、重度のハードウェア障害を示すトラップ、軽度のハードウェア障害を示すトラップ、ソフトウェアの障害を示すトラップ、停電による無停電電源への切り替えなどシステム障害ではないが環境的な障害に伴って発生するトラップなどいろいろな種類がある。全ての監視者が全てのトラップを監視するのではなく、情報システム部門の管理者はローカルのハードウェア・ソフトウェアのシステム全体を管理するため全てのトラップが必要だが、特定のソフトウェアの管理者はハードウェアの障害は知りたくないがソフトウェアの障害は知りたい、ソフトウェアの障害や停電などのシステムの障害を示さないトラップは必要ないメーカーのサポート部門など、監視者により知りたい障害の内容は異なる。

【0088】このような要求に対応するため、実施の形態5では電子メール送信先ごとにトラップの種類を選別して、その送信先に必要なトラップのみから構成される電子メールの本文を作成して送信する。

【0089】この発明の実施の形態に係わる障害通知方式は、コンピュータが、自身の状態を監視する監視ハードウェアからのトラップを受信した後、これまでに示した方法である程度障害を溜めてから一つの電子メールで監視者に送信する構成において、電子メールの送信先ごとに送信するトラップを予め設定したテーブルを持ち、電子メールを作成する時に送信先ごとに、対応するテーブルを検索してテーブルに存在するトラップから構成される電子メールを作成し、電子メールを送信するものである。

【0090】この実施の形態におけるシステム全体の構成は、従来の図29に示す構成と同じである。この実施の形態のコンピュータの構成は、図1に示される電子メール生成手段13を、図16で置き換えた構成となる。図16の54は複数のトラップを選別するための送信トラップ登録テーブルであり、それぞれに番号がついている。この番号は、送信トラップ登録テーブルを識別する識別子の一例である。53は各電子メールアドレスとトラップを選別するための送信トラップ登録テーブルの対応表(送信トラップ対応テーブル)であり、トラップ種類選別手段60は送信トラップ対応テーブル53と送信トラップ登録テーブル54から、トラップキューにあるトラップのどれをそのメール送信先のためのメール本文に含めるか決定する。そして、電子メール生成手段23により各電子メールアドレスごとにメール本文が作成される。

【0091】次に、動作について説明する。図17はトラップキューの内容を元にして各メール送信先に電子メールを送信するまでの処理を示すフローチャートである。これまでに示した実施の形態におけるメール送信直前の段階で、送信先の各メールアドレスに対してステッ

プST162, ST163, ST164, ST165, ST166で示される処理がそれぞれ行なわれる。

【0092】ステップST162において送信トラップ対応テーブル53から送信トラップ登録テーブル54の番号を求める処理が行なわれる。そして、ステップST163においてトラップ種類選別手段60によりトラップキューに存在する全てのトラップに対して送信トラップ登録テーブル54の対応するテーブル番号に存在するトラップが選択されて、選択されたトラップのリストが作成される。ステップST164において選択されたトラップのリストにトラップが存在するかどうか、即ち空でないかどうか判断する。トラップが存在する場合には、ステップST165において選択されたトラップのリストを元に電子メール生成手段23によりメール本文が作成される。メール本文の内容は図3と同じ内容となる。そして、ステップST166において対応する電子メールアドレスにメールが送信される。トラップが存在しない場合には電子メールを送信しない。そして、次のメールアドレスの処理に戻る。

【0093】この実施の形態により、各監視者ごとに監視したい障害のみが電子メールで送信され、監視の対象外の障害は送信されず、各監視者が監視の対象となるトラップと対象外のトラップを振り分ける手間が省けるため障害の解析の効率が上がる。また、監視の対象外のトラップはメールに含まれないためメールのサイズは小さくなり、また、監視の対象のトラップがない場合にメールは送信されないため、通信のトラフィックを削減できるという効果が得られる。

【0094】以上のように、この実施の形態においては、上記コンピュータにおいて、発生した障害の内容を電子メールで監視者に通知する際に、トラップ発生後すぐに電子メールを送信せず、これまでに示した方法である程度トラップを溜めてから一つの電子メールで送信する構成において、監視者の電子メールの送信先ごとに送るべきトラップを設定できる事を特徴とする障害通知方式について説明した。

【0095】実施の形態6. コンピュータで発生する障害によってはトラップの発生が連続して止まらなくなる場合がある。このような障害が発生すると、トラップに伴う障害の電子メールが監視者に連続して送信される。このためネットワークや途中の中継メールサーバに過大な負荷を与える事になる。この異常な状態はコンピュータがダウンするか、人手によりコンピュータを停止するか、障害を取り除くまで続く。特に夜中など監視者が不在の場合には、対応が遅れて多大な被害が出る可能性がある。実施の形態6はこの問題を解決するものである。

【0096】この発明の実施の形態に係わる障害通知方式は、トラップの発生が一定の時間間隔以内に起こる状態が一定時間継続したことを検出するトラップ頻発状態検出手段と、逆にトラップが発生しない状態が一定時間

継続したことを検出するトラップ停止状態検出手段とを備え、トラップ頻発状態を検出した際に、電子メールによる障害通知を一時停止するとともに、障害通知を一時停止したことを電子メールで監視者に知らせる、逆にトラップ停止状態を検出した際に、電子メールによる障害通知を再開するとともに、障害通知を再開したことを電子メールで監視者に知らせるものである。

【0097】この実施の形態におけるシステム全体の構成は、従来の図29に示す構成と同じである。コンピュータの構成は図1に示されるトラップ検出手段12を、図18で置き換えた構成となる。図18のトラップ検出手段12aは、状態変数71の値がONの場合のみトラップを検知して、状態変数71の値がOFFの場合にはトラップを検知しない。トラップ検知の停止・再開を制御するトラップ検知制御手段は、トラップが継続しているかを示す状態変数72と、継続状態を数えるカウンタ73と、設定されたタイマー値で定期的にタイマーイベントを出すタイマー74と、タイマーの間隔を設定するタイマー値設定手段75から構成される。図19は、この実施の形態におけるタイマー、カウンタの動作を制御する定数値を示す図である。これらの定数値は、図18の定数値記憶部77に保持される。

【0098】次に、トラップ検知の停止・再開を制御するトラップ検知制御手段70の動作について説明する。図20、図21はトラップ検知制御手段の状態遷移図である。初期化の段階でS170にてカウンタ73が"0"にセットされて、状態がS179の中のS171に移行する。同時にタイマー間隔が図19のTrapUnitTimeに設定されタイマー74が開始する。この時、状態変数72は"0"、状態変数71は"ON"となる。状態S171においてトラップイベントが発生した場合には、状態S172のトラップが継続している状態に移行し、状態変数72が"1"になる。この状態でさらにトラップイベントが発生すると状態は移行せずS172のままとなる。タイマー74によるタイマーイベントが発生するとS175でカウンタ73の値が"1"増加してS171の状態に戻る。状態S171においてタイマーイベントを受信すると、S174によりカウンタ73が"0"に設定されて再びS171に戻る。

【0099】トラップの発生が長時間継続すると、状態遷移はS171→S172、TrapUnitTimeの時間経過後にS172→S175→S171を繰り返す、カウンタ73の値はその度に"1"増加する。状態S172においてタイマーイベントを受信すると、S174によりカウンタ73が"0"に設定されて再びS171に戻る。S175においてカウンタ73が図18に示したTrapMaxCountに達すると、S179→S177→S173の状態遷移が起こる。この時、状態変数71が"ON"→"OFF"に変化してトラップの検知を行わない状態になる。S177でトラップを

停止した事がトラップ検知手段12aに通知される。トラップ検知手段12aは、トラップの検知を停止したことを監視者に電子メールで送信する。トラップの検知を停止した事が電子メールで送信されて、タイマー値設定手段75によりタイマー間隔がTrapResumeTimeに変更される。

【0100】状態S173においては、トラップイベントが発生すると、状態遷移S173→S178→S173が発生して、S178でタイマーの残り時間がTrapResumeTimeに戻される。従って、トラップイベントが発生する間隔がTrapResumeTimeより大きくなるとタイマーイベントが発生しない。

【0101】状態S173において、トラップの発生が治まってTrapResumeTimeの時間が経過すると、タイマーイベントが発生して、状態遷移S173→S176→S171が発生する。この時S176においてトラップ再開がトラップ検出手段12aに通知される。トラップ検出手段12aは、トラップの検出を再開した事を電子メールで送信する。トラップの検出を再開した事が電子メールで送信されると、タイマー値設定手段75によりタイマー間隔がTrapUnitTimeに変更される。また、状態変数71は"ON"になりトラップの検知を行なう状態を示すようになり、状態変数72は"0"となる。

【0102】このように構成する事により、トラップの発生がTrapUnitTimeの時間以内に発生する状態がTrapMaxCount回継続するとトラップの検知が停止される。トラップの発生が止まらなくなる場合にも、約TrapUnitTime×TrapMaxCountの時間の経過後にはトラップの検知をやめるため電子メールは送信されなくなり、無限に電子メールが送信される事を防ぐことができる。また、障害の原因が一時的なもので自動的に障害から回復した場合には、TrapResumeTimeの時間経過後に再びトラップを検知して電子メールを送信できる状態に戻るという効果がある。

【0103】以上のように、この実施の形態では、上記コンピュータにおいて、障害によるトラップの発生が一定の時間間隔以内に起こる状態が一定時間継続した際に、電子メールによる障害通報を一時停止し、代わりに監視者には通報を一時停止したことを示す電子メールを送り、その後障害が発生しない状態が一定時間継続した際に、電子メールによる障害通報を再開するとともに、監視者に障害通報を再開したことを示す電子メールを送ることを特徴とする障害通知方式について説明した。

【0104】次に、この実施の形態の変形例について説明する。実施の形態6では障害が継続してトラップが止まらなくなると、全てのトラップの検知をやめてしまうため、継続しているトラップ以外の障害が発生しても検

出する事ができないという問題がある。

【0105】この問題点を解決するために、トラップ全体の検出を停止するのではなく、継続して発生しているトラップについてのみ検出を停止・再開して、その他のトラップについては影響なく障害の検出を行なう事を考える。

【0106】この発明の実施の形態に係わる障害通知方式は、特定のトラップの発生が一定の時間間隔以内に起こる状態が一定時間継続したことを検出するトラップ頻発状態検出手段と、逆に特定のトラップが発生しない状態が一定時間継続したことを検出するトラップ停止状態検出手段とを備え、特定のトラップの頻発状態を検出した際に、電子メールによる特定のトラップの検知を一時停止するとともに、特定のトラップの検知を一時停止したことを電子メールで監視者に知らせる、逆に特定のトラップ停止状態を検出した際に、特定のトラップの検知を再開するとともに、特定のトラップの検知を再開したことを電子メールで監視者に知らせるものである。

【0107】図22は図17の実施の形態6を各トラップごとに検知の停止・再開を行なえるようにした構成である。各トラップの制御テーブル76は、各トラップごとについての状態を制御する。制御テーブル76には障害が継続してトラップが止まらなくなる可能性のあるトラップに対応する、トラップの変数アドレスと、トラップの検知をON/OFFする状態と、トラップが継続しているかを示す状態と、トラップが継続している回数を示すカウンタ値と、対応するタイマーの番号が示されている。制御テーブル76に登録されている各トラップに対応して、74aのタイマー0～タイマーnまでのタイマーがある。トラップ検知手段12bは各トラップの制御テーブル76に登録されているトラップについて、トラップごとに検知の“ON/OFF”を判断して、トラップを検出する。検知の“ON/OFF”が“ON”の場合のみ、そのトラップを検知し、検知の“ON/OFF”が“OFF”の場合にはそのトラップが発生しても無視する。

【0108】次に、動作について述べる。図23、図24はトラップ検知制御手段の状態遷移図である。図25はトラップ検知手段12bのトラップ発生から、トラップの検知、あるいは、無視するまでの判断方法を示したフローチャートである。ステップST190にてトラップが発生すると、ステップST191にてトラップの変数アドレスが各トラップの制御テーブル76に存在するかどうかを検索する。存在しない場合にはステップST195にてトラップを検知する。存在する場合にはステップST193にて制御テーブル76の検知のON/OFFの行のトラップに対応する列を調べる。ONの場合にはトラップを検知する。OFFの場合にはトラップを検知しない。

【0109】トラップ検知の停止・再開を制御する手段

の動作は、図23から図24の21の状態遷移図により示される。各トラップの制御テーブル76に存在する全てのトラップについて、それぞれ、図23、図24に示す状態遷移が行われる。状態遷移の方法は図20と同一であるので詳細な説明は省略する。

【0110】このような構成により、制御テーブル76に存在する特定のトラップの発生が長時間継続した場合に、自動的に特定のトラップに関する電子メールを監視者に送信し続けるのを防ぎ、その他のトラップについては継続して監視できるという効果がある。また、特定のトラップに対する障害が治まった場合に、一定に時間経過後自動的にその特定トラップを監視可能に戻す効果がある。

【0111】以上のように、この実施の形態では、上記コンピュータにおいて、あらかじめ登録しておいた特定のトラップを伴う障害の発生が一定の時間間隔以内に発生する状態が一定時間継続した際、その特定のトラップの障害通報を一時停止して、かわりに監視者にはそのトラップに関する通報を停止した事を示す電子メールを送る。なお、その特定のトラップ以外は停止しない。その後、そのトラップの障害が発生しない状態が一定時間継続した際に、電子メールによるそのトラップの通報を再開し、監視者に障害通報を再開したことを示す電子メールを送る事を特徴とする障害通知方式について説明した。

【0112】実施の形態7. コンピュータにある障害が発生しても、それが一時的であり短時間内に修復される場合は、障害の発生、修復を示すトラップが短い時間間隔で連続発生する。例を上げると、瞬停（停電後の復電）、RAID縮退後のホットスベアによる自動再構築開始、などが上げられる。これまでの実施例では、トラップ間の関係には着目しておらず、複数トラップの論理的な区切りを考慮していないため、場合によっては停電発生を示す電子メールが送られた後に、続けて復電を示す電子メールが送られ、監視者は両方のメールを見るまで瞬停であることを判断できないという問題がある。本実施例はこの問題を解決するものである。

【0113】この発明の実施の形態に係わる障害通知方式は、コンピュータの運用において、互いに関連があり、比較的短い時間内に連続して発生する可能性の高いトラップの対と、連続発生しなかったと判断できる時間間隔を登録しておく手段を備え、トラップの対の最初のトラップが発生した時に、予め登録した時間待って電子メールを送信し、監視者に知らせるものである。

【0114】この実施の形態におけるシステム全体の構成は、従来の図29に示す構成と同じである。図26は実施の形態7によるコンピュータの構成を示す図である。図26においても、コンピュータの状態を監視し、状態情報を保持する監視ハードウェア11と、監視ハードウェアからのトラップを受信するトラップ検知手段1

2と、受信したトラップを元に電子メールを作成する電子メール生成手段13と、作成した電子メールを監視者に送信する電子メール送信手段14と、トラップキュー20は、実施の形態1の図1に示す構成と同じである。図23の80は、互いに関連し連続して発生するトラップの対、例えば、障害トラップと修復トラップの対と、連続発生しなかったと判断する時間間隔を登録しておくトラップ対/時間間隔テーブルである。このトラップ対/時間間隔テーブル80には、例えば、障害トラップには、“停電”を示すトラップのアドレス、修復トラップには“復電”を示すトラップのアドレス、時間間隔には“10秒”等の時間を一組としてエントリされる。81はタイマーで、テーブル80のエントリ数分ある。

【0115】次に、動作について説明する。図27はトラップ検知手段12がトラップを受信してから、電子メールを送信するまでの処理を示すフローチャートである。ステップST210で監視ハードウェアからのトラップを待つトラップ検知手段12が、ステップST211でトラップを受信すると、ステップST212で、まずトラップをトラップキュー20に追加する。

【0116】次に、ステップST213で、トラップ対/時間間隔テーブル80の障害トラップに受信したトラップと一致するエントリがあるか確認する。なければ、再び、ステップST210でトラップを待つ。ある場合はステップST214で、該当するエントリに登録されている時間間隔で対応するタイマー81を起動し、ステップST215で対応する修復トラップの発生、またはタイマーの満了を待つ。修復トラップが発生した場合は、ステップST216でYesとなり、ステップST217で修復トラップを含む電子メールを作成し、ステップST218でトラップキューをクリアした後、ステップST219で電子メールを送信する。修復トラップが発生せず、タイマーが満了した場合はステップST220で障害トラップまでの電子メールを作成し、ステップST218でトラップキューをクリアした後、ステップST219で電子メールを送信する。なお、ステップST218のトラップキュー20のクリアと、ステップST219の電子メール送信は順序を逆にして処理しても構わない。

【0117】このように構成することにより、監視者は一つの電子メールを見ることで、一つのまとまった事象が発生したことを容易に認識することができるという効果が得られる。また障害が短時間内に修復されない場合でも一定時間後に障害情報のみを含んだ電子メールが送られ、障害の発生を見落とすことが無いという効果も得られる。

【0118】以上のように、この実施の形態では、上記コンピュータにおいて、あるトラップ発生に対し、比較的短い時間内に続くトラップの発生が予想されるものについて、それらが対で一つの論理的な障害または事象を

表す場合は分割せずまとめて一つのメールで通知を行なう事の特徴とする障害通知方式について説明した。

【0119】実施の形態8. コンピュータにある障害が発生しても、それが一時的であり短時間内に修復される場合は、コンピュータの運転自体に支障は無く、監視者に通知する必要がない場合がある。例を上げると、CPU (Central Processing Unit) 使用率が一時的に上限値を越えた場合、メモリ使用量が一時的に上限値を越えた場合、などが上げられる。これまでの実施例では、障害トラップ発生後、その継続時間に着目していないため、短い時間一時的にCPUの使用率が上限値を越えただけでも、監視者に処置する必要の無い電子メールが送られるという問題がある。本実施例はこの問題を解決するものである。

【0120】この発明の実施の形態に係わる障害通知方式は、コンピュータの運用において、障害の発生に対し自動的な修復が期待できる事象について、障害トラップと修復トラップの対、および自動修復が望めないと判断できる時間間隔を登録しておく手段を備え、障害トラップが発生した時に、予め登録した時間待っても修復トラップが来ない場合に電子メールを送信し、監視者に知らせるものである。

【0121】この実施の形態におけるシステム全体の構成は、従来の図29に示す構成と同じである。また、コンピュータの構成は実施の形態7の図26と同じである。ただし、トラップの対の意味と時間間隔の意味が異なる。本実施例においては、図26の80は、互いに関連し連続して発生する障害トラップと修復トラップの対と、障害トラップ発生後、自動的な修復がもはや見込めないと判断する時間間隔とを登録しておくテーブルである。81はタイマーで、テーブル80のエントリ数分ある。

【0122】次に、動作について説明する。図28は、トラップ検知手段12がトラップを受信してから、電子メールを送信するまでの処理を示すフローチャートである。ステップST230で監視ハードウェアからのトラップを待つトラップ検知手段12が、ステップST231でトラップを受信すると、ステップST232で、まずトラップをトラップキュー20に追加する。

【0123】次に、ステップST233で、テーブル80の障害トラップに受信したトラップと一致するエントリがあるか確認する。なければ、再び、ステップST230でトラップを待つ。ある場合はステップST234で、該当するエントリに登録されている時間間隔で対応するタイマー81を起動し、ステップST235で対応する修復トラップの発生、またはタイマーの満了を待つ。修復トラップが発生した場合は、ステップST236でYesとなり、何もせずに再びステップST230でトラップを待つ。修復トラップが発生せず、タイマーが満了した場合は、ステップST237で障害トラップ

を含む電子メールを作成し、ステップST238でトラップキューをクリアした後、ステップST239で電子メールを送信する。なお、ステップST238とステップST239の処理は順序が逆でもよい。

【0124】このように構成することにより、監視者は、自動的に復旧し得る障害であって処置する必要の無い、一時的な障害発生を示す不要な電子メールを受信することが無いという効果が得られる。また障害が自動的に復旧し得る障害であっても、一定時間のうちに自動的に復旧せず、処置が必要な場合にのみ電子メールが送られるという効果も得られる。

【0125】以上のように、この実施の形態では、上記コンピュータにおいて、ある障害によるトラップ発生に対し、ある程度時間が経てば自動的に修復されることが予想されるものについて、障害が発生してから一定時間に修復されなかった場合に初めて障害とみなして通知を行なう事の特徴とする障害通知方式について説明した。

【0126】

【発明の効果】この発明によれば、トラップ受信後、トラップキューにまとめてから電子メールが送られるため、トラップが複数発生しても電子メールが複数送られることなく、メールサーバ、ネットワークに余計な負荷をかけることが無いという効果が得られる。またトラップキューを用いているため、電子メールに含まれるトラップの発生順序が失われずに監視者に通知され、監視者の解析を容易にする効果がある。

【0127】この発明によれば、トラップ受信後タイマー猶予時間待ってから電子メールが送られるため、トラップが短い時間内に連続で発生しても電子メールが複数送られることなく、メールサーバ、ネットワークの負荷を軽減するという効果が得られる。

【0128】この発明によれば、トラップ受信後、障害の後処理の完了するまでの間待ってから電子メールが送られるため、トラップが連続で発生しても電子メールが複数送られることなく、メールサーバ、ネットワークの負荷を軽減するという効果が得られる。

【0129】この発明によれば、トラップがまばらな間は猶予時間が小さくなり、猶予時間による通知の即時性が失われることを防ぐ効果が得られ、逆にトラップが短い時間間隔で連続発生する場合は、猶予時間が長くなり、監視者にメールが分割されて送られることが発生し難くなる効果がある。

【0130】この発明によれば、トラップが一定の数たまってから電子メールが送られるため、1通の電子メールに含まれるトラップの数は一定の数になり、多くのトラップを含む、極端にデータ量の大きなメールにより中継するメールサーバをダウンさせる危険を防ぐ事ができる効果がある。

【0131】この発明によれば、障害通報の電子メールに含まれるトラップの数は上限より多くなる事はな

め、極端に大きな電子メールが送信される事がなく、また、トラップの数が上限に達しない場合にも一定の時間の経過後に障害内容をまとめた電子メールを送信できるという効果がある。

【0132】この発明によれば、監視者に早く通知すべき重大なトラップが発生すると、その障害値が大きいためすぐに一定値を越えることとなり、監視者に早く通知が行われる効果がある。

【0133】この発明によれば、監視者毎に電子メールを送信する障害合計値を変えておけば、例えば、障害発生毎に処置の必要な情報システム部門の管理者には早く電子メールが送信され、迅速に処置が行えるようになるとともに、全社の管理者には障害がある程度まとまった段階で適切な頻度で電子メールが送信されるという効果がある。

【0134】この発明によれば、重障害を示すトラップを受信した場合には、すぐに監視者に電子メールが送信され、重障害によるシステムダウンの前に通知できる可能性が高くなる効果がある。

【0135】この発明によれば、各監視者ごとに監視したい障害のみが電子メールで送信され、監視の対象外の障害は送信されず、各監視者が監視の対象となるトラップと対象外のトラップを振り分ける手間が省けるため障害の解析の効率が上がる。また、監視の対象外のトラップはメールに含まれないためメールのサイズは小さくなり、監視の対象のトラップがない場合にメールは送信されないため通信のトラフィックを削減できるという効果がある。

【0136】この発明によれば、トラップの発生が一定の時間以内に発生する状態が一定回継続するとトラップの検知が停止され、トラップの発生が止まらなくなる場合にも、一定の時間の経過後にはトラップの検知をやめるため電子メールは送信されなくなり、無限に電子メールが送信される事を防ぐことができる。

【0137】また、この発明によれば、障害の原因が一時的なもので自動的に障害から回復した場合には、一定の時間経過後に再びトラップを検知して電子メールを送信できる状態に戻るという効果がある。

【0138】この発明によれば、制御テーブル76に存在する特定のトラップの発生が長時間継続した場合に、自動的に特定のトラップに関する電子メールを監視者に送信し続けるのを防ぎ、その他のトラップについては継続して監視できるという効果がある。

【0139】この発明によれば、監視者は一つの電子メールを見ることで、一つのまとまった事象が発生したことを容易に認識することができるという効果がある。さらに、障害が短時間内に修復されない場合でも一定時間後に障害情報のみを含んだ電子メールが送られ、障害の発生を見落とすことが無いという効果もある。

【0140】この発明によれば、監視者は、自動的に復

旧し処置する必要の無い、一時的な障害発生を示す不要な電子メールを受信することが無いという効果がある。さらに、障害が一定時間のうちに自動的に復旧せず、処置が必要な場合にのみ電子メールが送られるという効果もある。

【図面の簡単な説明】

【図 1】 この発明の実施の形態 1 における構成を示す図である。

【図 2】 この発明の実施の形態 1 におけるフローチャートである。

【図 3】 この発明の実施の形態 1、2、3、4、5、6、7、8 における障害の内容を示す電子メール本文である。

【図 4】 この発明の実施の形態 1 において障害が発生した際に前回の障害発生からの経過時間を記録しておき、その時間の逆数に比例する時間を利用する改良を行なう構成を示す図である。

【図 5】 この発明の実施の形態 1 におけるタイマー値決定手段 22 のフローチャートである。

【図 6】 この発明の実施の形態 2 におけるトラップの数が制限値に達した場合に電子メールを送信する構成を示す図である。

【図 7】 この発明の実施の形態 2 におけるフローチャートである。

【図 8】 この発明の実施の形態 2 においてトラップの数が制限値に達した、あるいは、タイマーが満了した場合に電子メールを送る改良を行なった構成を示す図である。

【図 9】 この発明の実施の形態 2 においてトラップの数が制限値に達した、あるいは、タイマーが満了した場合に電子メールを送る改良を行なった場合のフローチャートである。

【図 10】 この発明の実施の形態 3 における構成を示す図である。

【図 11】 この発明の実施の形態 3 におけるフローチャートである。

【図 12】 この発明の実施の形態 3 において監視者ごとにメールを送信する障害の重みの合計値を変化させる改良を行なった構成を示す図である。

【図 13】 この発明の実施の形態 3 において監視者ごとにメールを送信する障害の重みの合計値を変化させる改良を行なった場合のフローチャートである。

【図 14】 この発明の実施の形態 4 における重障害を示すトラップのテーブルである。

【図 15】 この発明の実施の形態 4 におけるフローチャートである。

【図 16】 この発明の実施の形態 5 における電子メール生成手段に相当する構成を示す図である。

【図 17】 この発明の実施の形態 5 におけるフローチャートである。

ャートである。

【図 18】 この発明の実施の形態 6 における構成を示す図である。

【図 19】 この発明の実施の形態 6 におけるタイマー、カウンタの動作を制御する定数値を示す表である。

【図 20】 この発明の実施の形態 6 におけるトラップ検知の停止・再開を制御する手段の状態遷移図である。

【図 21】 この発明の実施の形態 6 におけるトラップ検知の停止・再開を制御する手段の状態遷移図である。

10 【図 22】 この発明の実施の形態 6 についてトラップが頻発した状態を検知した時に頻発したトラップのみトラップ検知の停止・再開できるように改良した場合の構成を示す図である。

【図 23】 この発明の実施の形態 6 について各トラップごとにトラップ検知の停止・再開を制御する手段の状態遷移図である。

【図 24】 この発明の実施の形態 6 について各トラップごとにトラップ検知の停止・再開を制御する手段の状態遷移図である。

20 【図 25】 この発明の実施の形態 6 について図 22 におけるトラップ検知手段 12b のフローチャートである。

【図 26】 この発明の実施の形態 7、8 における構成を示す図である。

【図 27】 この発明の実施の形態 7 におけるフローチャートである。

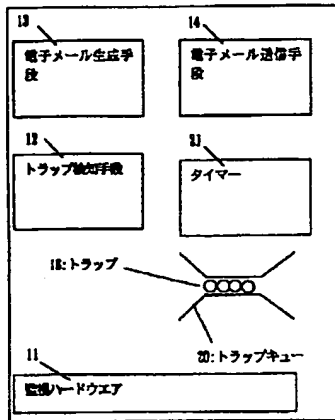
【図 28】 この発明の実施の形態 8 におけるフローチャートである。

30 【図 29】 従来の電子メールによる障害通知方式の構成を示す図である。

【符号の説明】

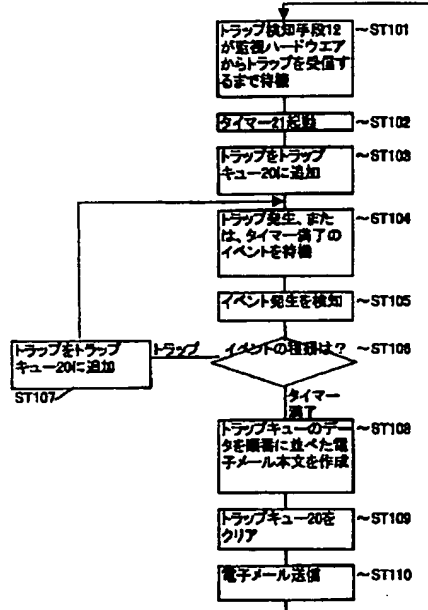
1a コンピュータ（監視対象コンピュータ）、2a、2b メールサーバ、3a 管理 PC、4a、4b LAN、4c LAN/WAN/Internet、11 監視ハードウェア、12、12a、12b トラップ検知手段、13 電子メール生成手段、14 電子メール送信手段、20、20a、20b、…20n-1、20n トラップキュー、21 タイマー、22 タイマー値決定手段、30 カウンタ、41 障害値加算手段、40 51 送信先テーブル、52 重障害トラップテーブル、53 送信トラップ対応テーブル、54 送信トラップ登録テーブル、61 電子メールの本文、70、70b トラップ検知制御手段、71 トラップの検知を行なうか行わないかを示す状態変数、72 トラップが継続しているかどうかをしめす状態変数、73 継続状態を数えるカウンタ、74、74a 設定されたタイマー値で定期的にイベントを出すタイマー、75 タイマー値設定手段、80 トラップ対/時間間隔テーブル、81 タイマー。

【図1】



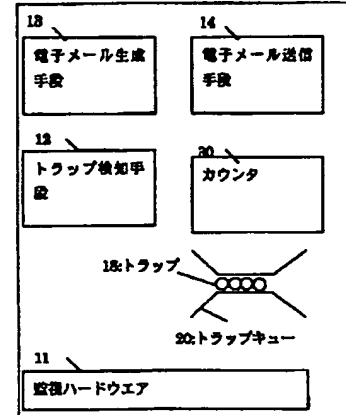
実施の形態1の構成図

【図2】



実施の形態1のフローチャート

【図6】



実施の形態2の構成図

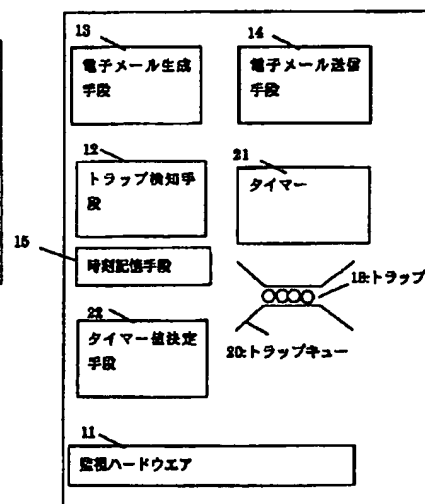
【図3】

61:電子メールの本文

発生時刻 ~62	宛先アドレス ~63	変数値 ~64
1999/5/17 20:15:30	0x000A	01
1999/5/17 20:15:31	0x0080	00
1999/5/17 20:15:40	0x0081	10000
1999/5/17 20:15:50	0x007A	00
1999/5/17 20:16:10	0x1002	01
1999/5/17 20:16:11	0x046B	02
1999/5/17 20:16:12	0x05BA	100000

電子メールの本文の内容

【図4】



実施の形態1の他の例

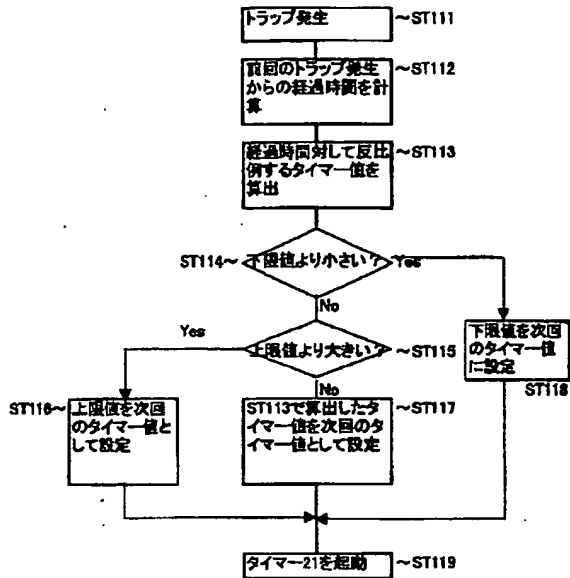
【図14】

62:重層トラップテーブル

トラップのアドレス
0x0010 ~521
0x0645 ~522
...

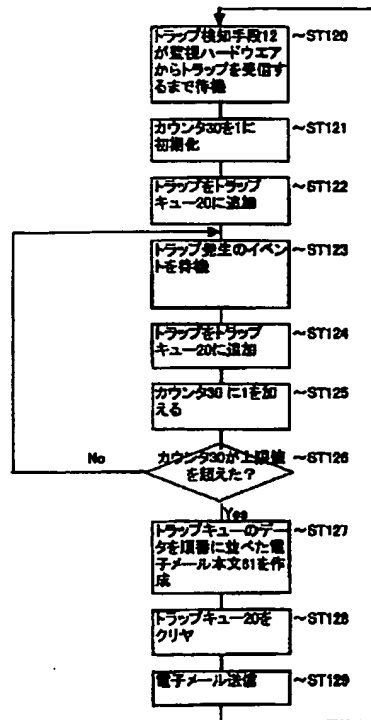
【図5】

(図2のST102が以下の処理と置き換わる)



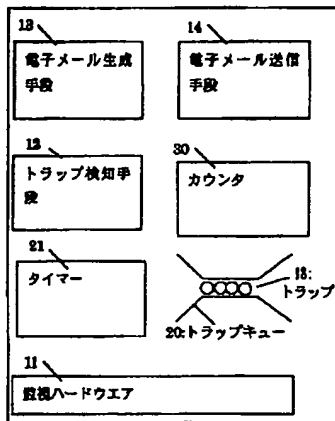
タイマー値決定手段(22)のフローチャート

【図7】



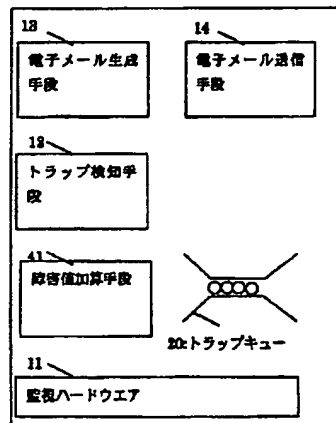
実施の形態2のフローチャート

【図8】



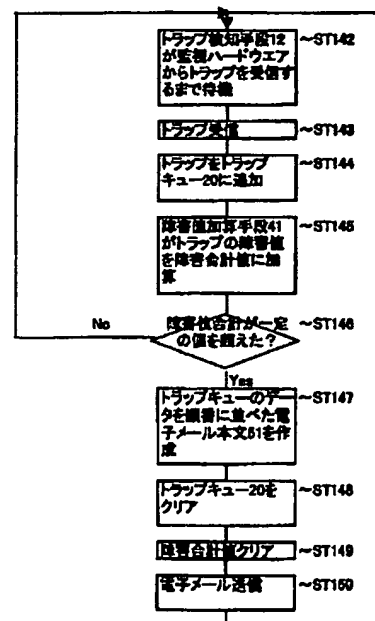
実施の形態2の他の例

【図10】



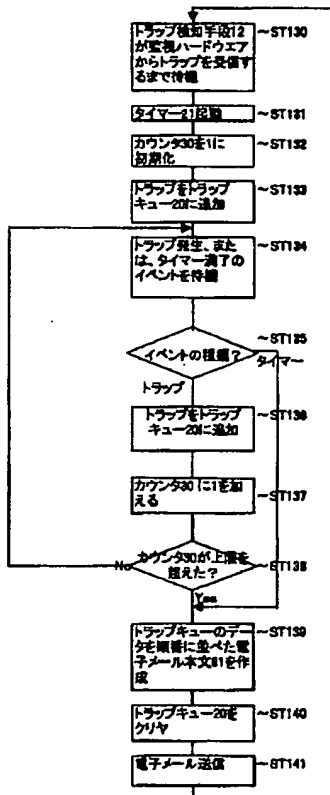
実施の形態3の構成例

【図11】



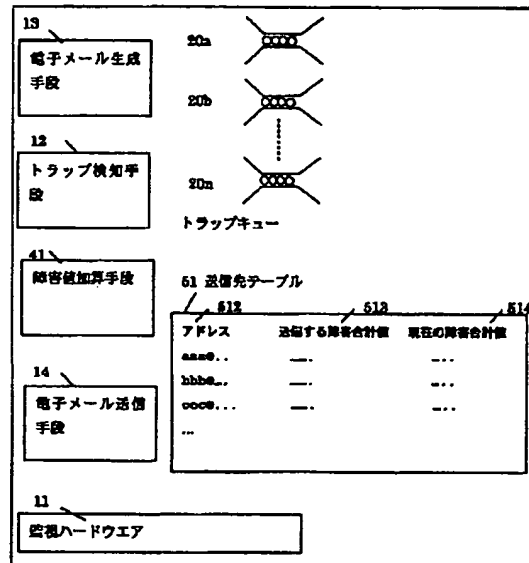
実施の形態3のフローチャート

【図9】



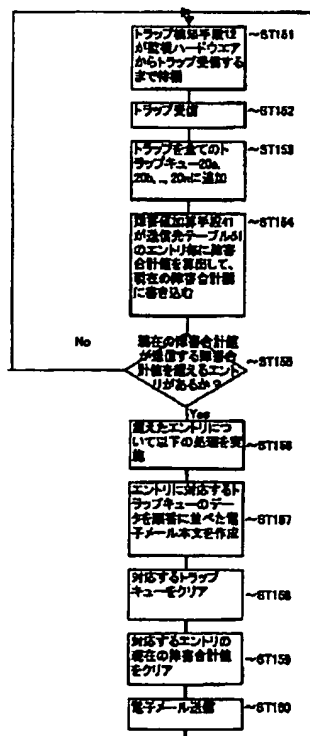
実施の形態2の他の例のフローチャート

【図12】



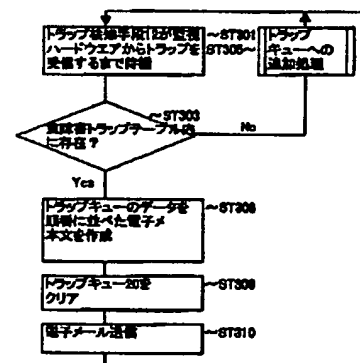
実施の形態3の他の例

【図13】



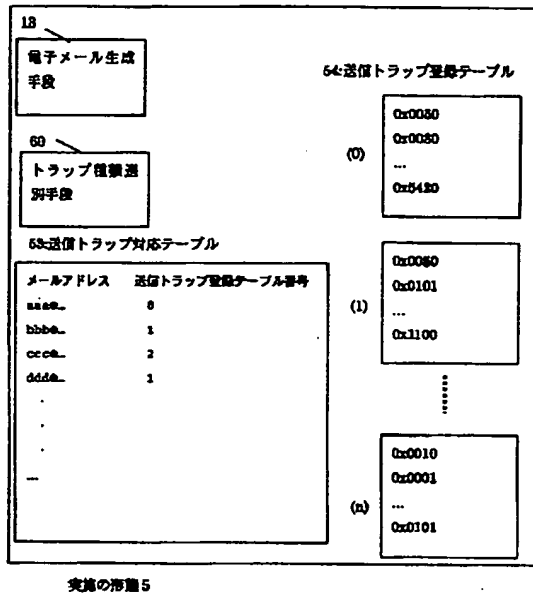
実施の形態3の他の例のフローチャート

【図15】



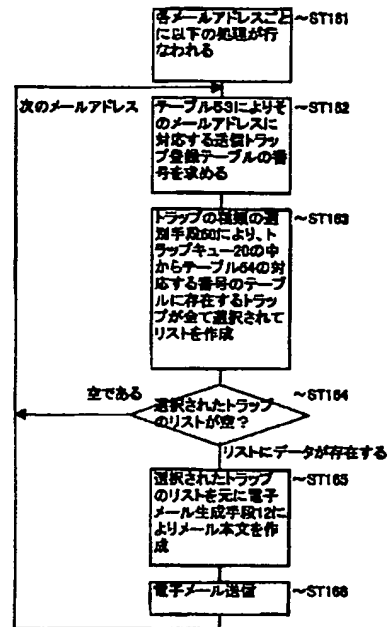
実施の形態4のフローチャート

【図16】



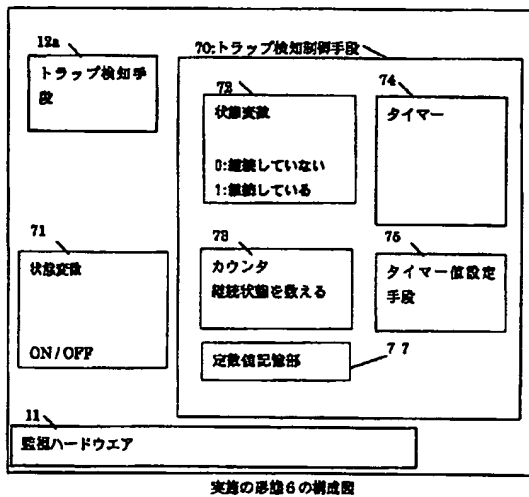
実施の形態5

【図17】



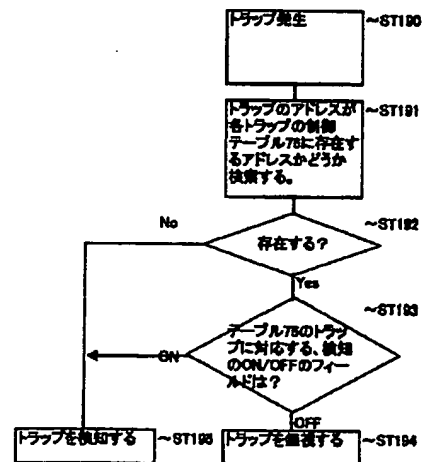
実施の形態5のフローチャート

【図18】



実施の形態6の構成図

【図25】



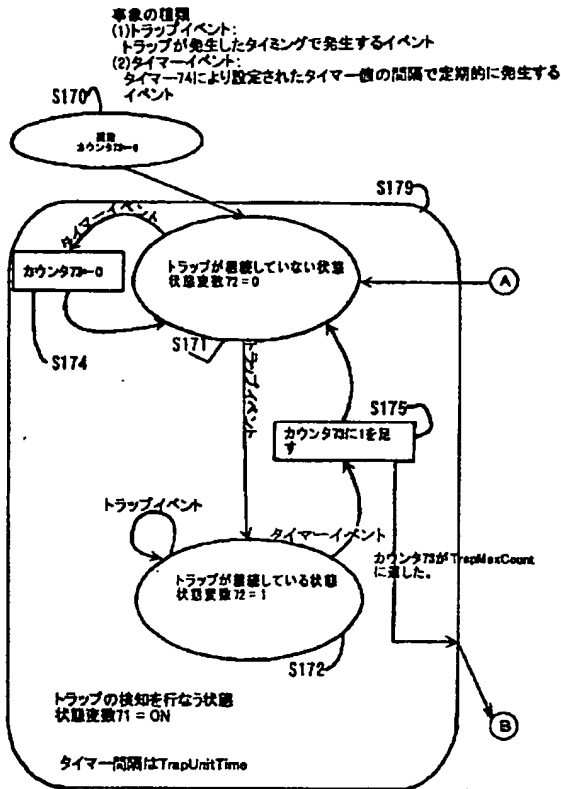
トラップ検知手段12bのフローチャート

【図19】

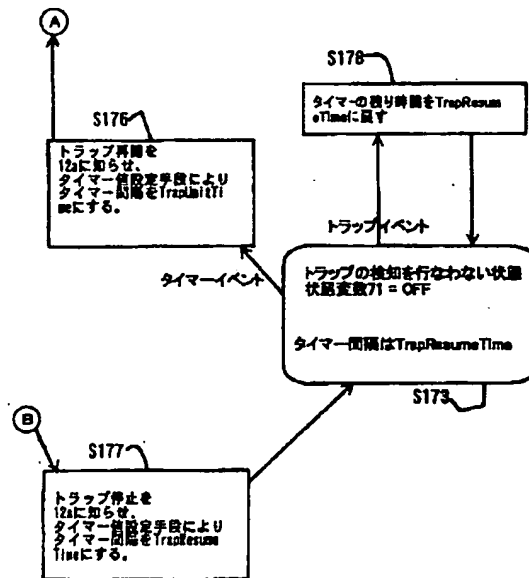
TrapUnitTime:	トラップの検知を行なう状態におけるタイマー値
TrapResumeTime:	トラップの検知を行わない状態におけるタイマー値
TrapMaxCount:	カウンタ73の最大値

実施の形態6におけるタイマー、カウンタの動作を制御する定数値

【図 20】

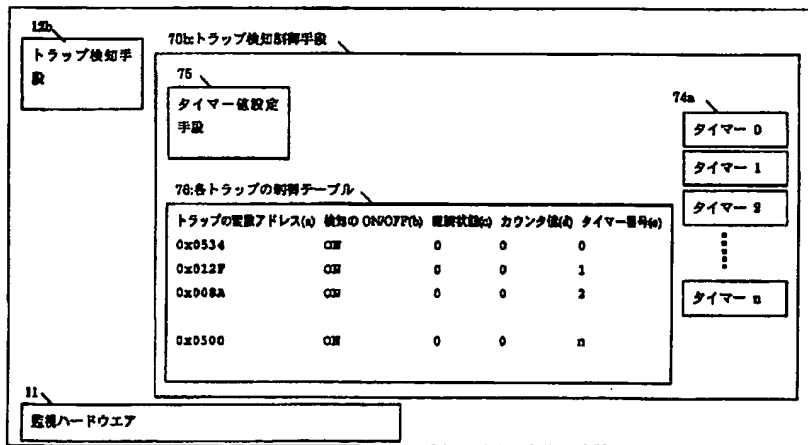


【図 21】



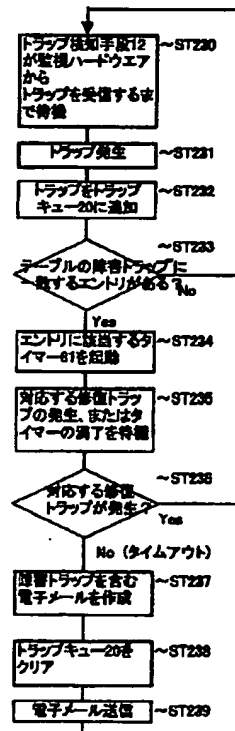
実施の形態 6 (トラップ検知制御手段の状態遷移図)

【図 22】



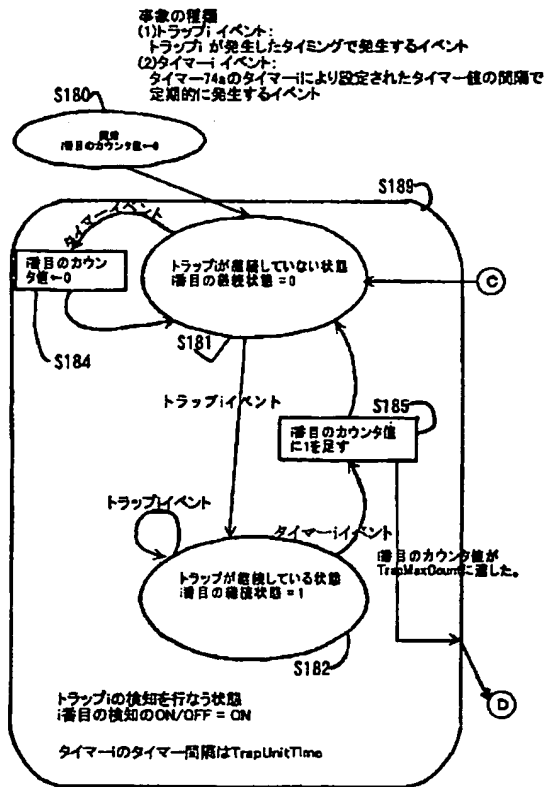
実施の形態 6 の他の例

【図 28】

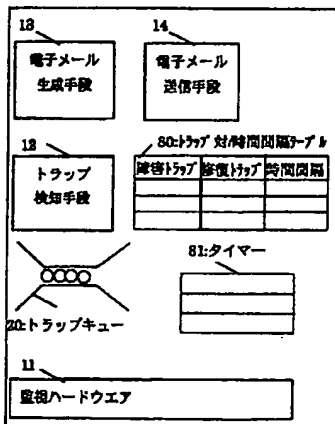


実施の形態 6 のフローチャート

【図23】

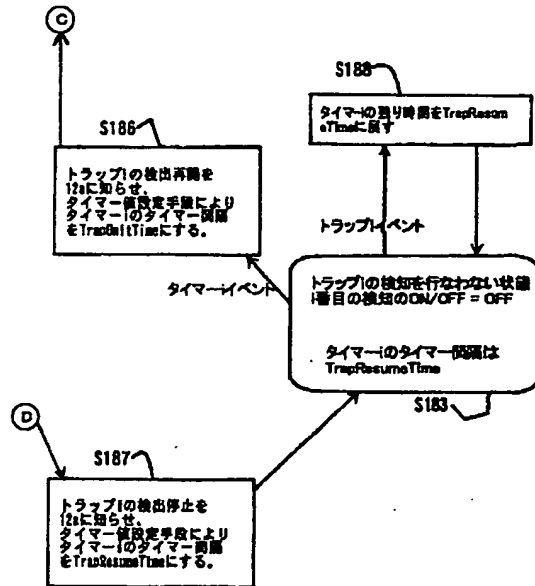


【図26】

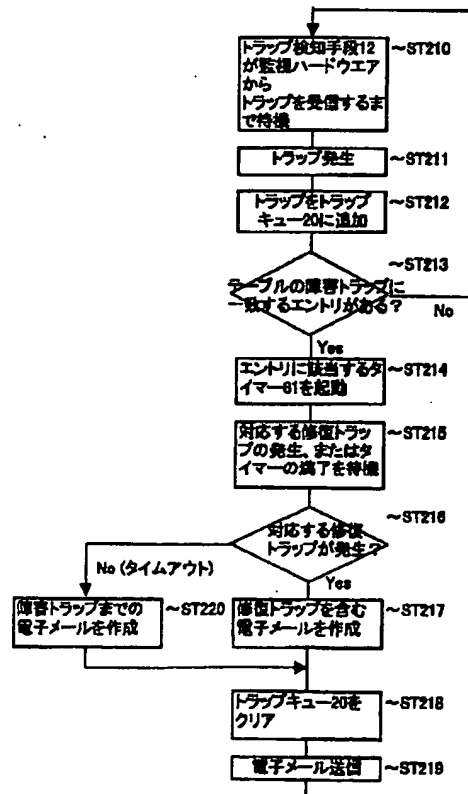


実施の形態7, 8の構成図

【図24】

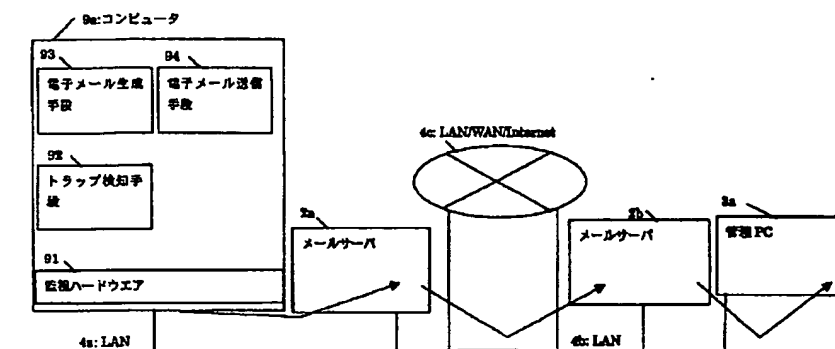


【図27】



実施の形態7のフローチャート

【図29】



フロントページの続き

(51) Int. Cl.⁷

H 0 4 L 12/58

識別記号

F I

テーマコード(参考)

Fターム(参考) 5B089 GA23 GB02 JA31 JA35 JB17

KA07 KA12 KC15 KC28 KC29

KC39 LA03 LA06

5K030 GA12 HA06 HB00 JA10 KA21

KX11 MB01

9A001 CC02 CC08 JJ14 JJ25 LL05

LL09

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.